WHAT IS CLAIMED IS:

1. A cryptographic key distribution method at a cryptographic key distribution apparatus in which a sender transmits signal light to a receiver through an optical transmission channel, wherein:

said sender, comprising the steps of:

setting light intensity and a modulation index of outputting signal light so that the signal to noise ratio (SNR) of an eavesdropper is smaller than 2 dB even when said eavesdropper eavesdrops at the sending end by using any receiving equipment and also the SNR of said receiver at the receiving end is larger than −10 dB; and

transmitting signal light modulated by modulation signals that a random number sequence was coded, and

said receiver, comprising the steps of:

receiving said signal light of said random number sequence transmitted from said sender;

calculating the probability distributions by using the frequency (occurrence times) distributions of said received signal light having fluctuation caused by that noise was added;

judging whether said eavesdropper exists or not based on changes of said probability distributions, and also setting a discrimination threshold value so that the error rate of said receiver is 5% or less;

discriminating the bit value of each bit in said random number sequence based on said discrimination threshold value; and

informing said sender of the positions of bits that said receiver could discriminated, and taking out only the bit sequence having no errors in the discrimination, and sharing said bit sequence having no errors with said sender, and wherein:

said shared bit sequence is made to the cryptographic key.

2. A cryptographic key distribution method in accordance with claim 1, wherein:

the random number using in said random number sequence is a binary random number, and said calculated probability distributions have a peak respectively (that is, two peaks) corresponding to said binary number at said receiving end, and the binary random number sequence is coded so that said calculated probability distributions become the probability distributions being symmetry each other.

3. A cryptographic key distribution method in accordance with claim 2, wherein:

Manchester codes are used for coding said binary random number.

4. A cryptographic key distribution method in accordance with claim 2, wherein:

it is confirmed that said calculated probability distributions have said peak respectively (that is, two peaks) and are symmetry corresponding to said binary number (0,1), and when such probability distributions are not confirmed, it is judged that said eavesdropper exists at said cryptographic key distribution, and the distribution of said cryptographic key is stopped and a fresh cryptographic key is distributed again.

5. A cryptographic key distribution method in accordance with claim 1, wherein:

when said cryptographic key is distributed, management information composed of clock signals, said light intensity and said modulation index of said transmitting signal light is transmitted to said

receiver by using a transmission channel being independent of said optical transmission channel for said cryptographic key distribution.

6. A cryptographic key distribution method in accordance with claim 5, wherein:

said receiver calculates a light intensity expectation value of receiving signal light, estimating from received light intensity information of said sending end and a known transmission channel loss, and compares said calculated result with the light intensity of actually received signal light, and judges an abnormal state of said optical transmission channel based on the difference between said calculated value and said actually received value, and decides to stop distributing said cryptographic key based on said judged result.

7. A cryptographic key distribution apparatus, comprising:

a transmitting apparatus that radiates signal light modulated by a coded random number sequence;

an optical transmission channel that transmits said signal light radiated from said transmitting apparatus; and

a receiving apparatus that receives said signal light transmitted through said optical transmission channel, and wherein:

said receiving apparatus decodes said signal light received through said optical transmission channel, and calculates the probability distributions from the frequency (occurrence times) distributions of decoded signals having fluctuation caused by that noise was added, and judges whether an eavesdropper exists or not based on changes of said probability distributions, and also sets a discrimination threshold value so that the error rate of said receiving apparatus is 5% or less, and discriminates a bit value of each bit of said random number sequence based on said discrimination threshold value, and transmits positions of

bits that said receiving apparatus could discriminate to said transmitting apparatus, and wherein:

an average number of photons N ($N \geqq 1$) per one pulse of said signal light radiating from said transmitting apparatus, a modulation index δ of said signal light radiating from said transmitting apparatus, and a transmission loss L at said optical transmission channel satisfy following equations.

$\delta \leqq 0.8 / N$

$2 \delta L^2 N^2 / Nn > 0.1$

In this, Nn signifies the noise level of the receiving apparatus.

8. A cryptographic key distribution apparatus in accordance with claim 7, wherein:

said transmitting apparatus, comprising:

a first light source;

a clock generator;

a random number generator that generates random numbers based on clocks generated by said clock generator;

an encoder that encodes said random numbers generated at said random number generator;

a first modulator that modulates light from said first light source based on signals encoded at said encoder and makes said modulated signals signal light;

an attenuator that attenuates light intensity of said signal light outputted from said first modulator to about a noise level;

a second light source that generates light using for clock light;

a second modulator that modulates light from said second light source based on clocks generated at said clock generator and makes said modulated signals clock light; and

a multiplexer that multiplexes said signal light outputted from

said attenuator and said clock light outputted from said second modulator and outputs said multiplexed light to said optical transmission channel, and

said receiving apparatus, comprising:

a wavelength de-multiplexer that divides received signals transmitted through said optical transmission channel into said signal light and said clock light;

a clock reproducer that converts said clock light inputted from said wavelength de-multiplexer into electric clocks;

a decoding detector that decodes said signal light inputted from said wavelength de-multiplexer and converts said decoded signal light into electric signals; and

an operating unit that measures the frequency (occurrence times) distributions of said electric signals having fluctuation caused by that noise was added from said decoding detector based on said clocks from said clock reproducer, and calculates the probability distributions from said frequency distributions, and judges whether an eavesdropper exists or not based on changes of said probability distributions, and sets said discrimination threshold value so that the error rate of said receiving apparatus is 5% or less, and discriminates a bit value of each bit of said random number sequence based on said discrimination threshold value, and transmits positions of bits that said operating unit could discriminate to said transmitting apparatus.

9. A cryptographic key distribution apparatus in accordance with claim 8, wherein:

said clock reproducer, comprising:

a light detector that converts said clock light into electric signals; and

a clock reproducing circuit that forms said electric signals from

said light detector into waveforms,

said decoding detector, comprising:

a 50%-50% wavelength de-multiplexer that divides said signal light inputted from said wavelength de-multiplexer into two components at the dividing ratio is 1 to 1;

a delay circuit that delays one of said signal light divided at said 50%-50% wavelength de-multiplexer; and

a balanced detector that converts the difference between said signal light inputted from said delay circuit and said signal light inputted from said 50%-50% wavelength de-multiplexer into electric signals.

10. A cryptographic key distribution apparatus in accordance with claim 8, wherein:

said encoder in said transmitting apparatus encodes said random number sequence so that said probability distributions calculated at said receiving apparatus has a peak respectively (that is, two peaks) corresponding to binary and are symmetry with each other.

11. A cryptographic key distribution apparatus in accordance with claim 7, wherein:

Manchester codes are used at coding said random number sequence.